METHOD AND APPARATUS TO PROVIDE ENCRYPTION AND AUTHENTICATION OF A MINI-PACKET IN A MULTIPLEXED RTP PAYLOAD

ABSTRACT

A method and apparatus to provide encryption and authentication of a mini-packet in a multiplexed real time protocol (RTP) payload. Mini-packets are assembled into a payload wherein each mini-packet includes an associated mini-header for ensuring proper processing of each mini-packet. Padding is added to mini-packets when the mini-packets are encrypted to insure each mini-packet is an integral multiple of a predetermined block size. Padding for each mini-packet is determined according to p=n-k*floor((n-1)/k), wherein p is the amount of padding added to each mini-packet, n is the actual data size, and k is the block size. The padding added to the data for each packet comprises p-1 units of padding and a final padding unit for indicating the amount of padding. An authenticator may also be added to each mini-packet. A length indicator is set in each mini-header for indicating a total length of the mini-packet including the authenticator. The authenticator may then be removed based upon knowing a type of authentication used for generating the authenticator.